IN THE CLAIMS

Please amend claims 1, 2, 4, 6-8, 14, 19, 20, and 23-33 as follows:

1.   (Currently Amended) A system to support management operations associated with an interconnect device, the system comprising:

a configuration switch <u>configured</u> to receive an operator command to reset authentication data that facilitates authorization of the management operations from an operator, and <u>configured</u> to generate a reset signal in response to the operator command; and

a port of the interconnect device, coupled to the configuration switch, <u>the port configured</u> to maintain the authentication data and to reset the authentication data upon receiving the reset signal from the configuration switch.

2.   (Current Amended) The system of claim 1 wherein the port is <u>configured</u> to store the authenticated data together with a set of associated attributes.

3.   (Original) The system of claim 2 wherein:

the port is a management port;

the authentication data is a management key; and

the set of associated attributes includes a protection attribute specifying a level of protection required for performing a particular management operation and an expiration attribute controlling expiration of the management key.

4.   (Currently Amended) The system of claim 3 further comprising:

a sub-network (subnet) manager, coupled to the interconnect device, <u>the subnet manager configured</u> to store a copy of the management key and to include the management key into a Subnet Management Packet (SMP) sent to the management port for a comparison with the management key stored in the management port.

9

5.   (Original) The system of claim 3 wherein the management port comprises:

an initialization module to store the authentication data;

a decoder to store a first copy of the authentication data;

a management agent to store a second copy of the authentication data; and

a processor subsystem interface to provide access to a storage device that stores a third copy of the authentication data.

6.   (Currently Amended) The system of claim 5 wherein the decoder is <u>configured</u> to receive the reset signal from the configuration switch.

7.   (Currently Amended) The system of claim 6 wherein the decoder is <u>configured</u> to communicate the reset signal to any one of the initialization module, the management agent and the configuration interface.

8.   (Currently Amended) A method to support management operations associated with an interconnect device, the method comprising:

receiving a reset signal from a configuration switch at a decoder of a management port, the reset signal indicating that an operator requested a reset of <u>an</u> authentication data that facilitates authorization of the management operations; and

resetting a copy of the authentication data, ~~that~~<u>wherein the authentication data</u> is stored in the decoder in response to the reset signal.   ,

9.   (Original) The method of claim 8 further comprising:

receiving a management packet from a sub-network (subnet) manager with an update value for the authentication data; and

setting the copy of the authentication data stored in the decoder to the update value.

10.   (Original) The method of claim 8 further comprising:

10

the decoder communicating the reset signal to any one of an initialization module, a
management agent and a processor subsystem interface; and

resetting a corresponding copy of the authentication data upon receiving the reset signal
at any one of the initialization module, the management agent and the processor subsystem
interface.

11.   (Original) The method of claim 8 wherein the authentication data is a management key.

12.   (Original) A method to support management operations associated with an interconnect
device, the method comprising:

detecting that a reset of authentication data residing in a management port of the
interconnect device is required;

informing an operator that the reset is required;

refraining from sending subnet management packets (SMPs) to the management port
upon detecting that the reset is required;

receiving a message from the operator that indicates that the authentication data has been
reset; and

subsequent to the receipt of the message, sending to the management port an update SMP
with a request to set authentication data residing in each unit of the interconnect device to an
update value.

13.   (Original) The method of claim 12 wherein:
the SMPs are virtual lane 15 (VL 15) packets; and
the authentication data is a management key.

14.   (Original) The method of claim 12 wherein:
each SMP sent to the management port includes authentication data that matches
authentication data residing in a decoder of the management port unless the authentication data
residing in the decoder is set to a predetermined value.

11

15.   (Original) The method of claim 12 wherein the authentication data is stored in the management port with a set of associated attributes, the set of associated attributes including a protection attribute specifying a level of protection required for performing a particular management operation and an expiration attribute controlling expiration of the authentication data.

16.   (Original) The method of claim 15 wherein detecting that the reset is required comprises:
        sending a SMP containing a copy of the authentication data maintained by the subnet manager to the management port; and
        receiving a trap indicating that the management port has invalidated the SMP due to a mismatch between the authentication data included the SMP and the authentication data maintained by the management port and further indicating that the expiration attribute is set to a value that prevents expiration of the authentication data.

17.   (Original) The method of claim 15 wherein detecting that the reset is required comprises:
        sending an initial SMP containing a copy of the authentication data maintained by the subnet manager to the management port;
        determining that a response to the initial SMP has not been received from the management port for a predefined time period;
        re-sending the initial SMP for a predetermined number of times without receiving a response; and
        determining that the failure to receive the response may be caused by a mismatch between the authentication data included in the initial SMP and the authentication data maintained by the management port.

18.   (Original) The method of claim 12 wherein the update value is the value of authentication data stored in a database of the subnet manager.

Amendment and Response
Applicant: Norman C. Chou et al.
Serial No.: 10/057,159
Filed: January 24, 2002
Docket No.: 10011314-1/A310.258.101
Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

19.   (Currently Amended) The method of claim 12 wherein:

the management port stores multiple copies of the authentication data; and

    only one copy from the multiple copies has been reset in response to the operator

command.

20.   (Currently Amended) The method of claim 19 further comprising:

    determining the update value for the update SMP.

21.   (Original) The method of claim 20 wherein determining the update value comprises:

    upon receiving the message indicating that the authentication data maintained by the

management port has been reset, sending to the management port a read SMP requesting a

current value of the authentication data maintained by the management port;

    receiving the current value of the authentication data maintained by the management port

from the management port;

    designating the received value as the update value; and

    updating authentication data in a database of the subnet manager with the received value.

22.   (Original) An apparatus to support management operations associated with an

interconnect device, the apparatus comprising:

    means for detecting that a reset of authentication data residing in a management port of

the interconnect device is required;

    means for informing an operator that the reset is required;

    means for refraining from sending subnet management packets (SMPs) to the

management port upon detecting that the reset is required;

    means for receiving a message from the operator that indicates that the authentication

data has been reset; and

    means for sending to the management port an update SMP with a request to set

authentication data residing in each unit of the interconnect device to an update value.

13

23.   (Currently Amended) A system comprising:

        an interconnect device to maintain authentication data in a plurality of units, the authentication data facilitating management operations associated with the interconnect device;

        a configuration switch, coupled to the interconnect device, the configuration switch configured to cause a reset of authentication data residing in a management port of the interconnect device; and

        a sub-network (subnet) manager, coupled to the interconnect device, the subnet manager configured to detect that the reset of authentication data residing in the management port is required, to inform an operator that the authentication data has been reset, and to send to the management port an update data packet with a request to set the authentication data residing in each of the plurality of units of the interconnect device to an update value.

24.   (Currently Amended) The system apparatus of claim 22 wherein:
the SMPs are virtual lane 15 (VL 15) packets;, and
the authentication data is a management key.

25.   (Currently Amended) The system apparatus of claim 22 wherein:
each SMP sent to the management port includes authentication data that matches authentication data residing in a decoder of the management port unless the authentication data residing in the decoder is set to a predetermined value.

26.   (Currently Amended) The system apparatus of claim 22 wherein the authentication data is stored in the management port with a set of associated attributes, the set of associated attributes including a protection attribute specifying a level of protection required for performing a particular management operation and an expiration attribute controlling expiration of the authentication data.

27.   (Currently Amended) The system of claim 2623 wherein the subnet manager is configured to detect that the reset is required by sending a subnet manager packet (SMP)

14

containing a copy of the authentication data maintained by the subnet manager to the management port, and receiving a trap indicating that the management port has invalidated the SMP due to a mismatch between the authentication data included the SMP and the authentication data maintained by the management port and further indicating that the expiration attribute is set to a value that prevents expiration of the authentication data.

28.   (Currently Amended) The system of claim 2623.wherein the subnet manager is configured to detect that the reset is required by sending an initial subnet management packet (SMP) containing a copy of the authentication data maintained by the subnet manager to the management port, determining that a response to the initial SMP has not been received from the management port for a predefined time period, re-sending the initial SMP for a predetermined number of times without receiving a response, and determining that the failure to receive the response may be caused by a mismatch between the authentication data included in the initial SMP and the authentication data maintained by the management port.

29.   (Currently Amended) The system of claim 2423 wherein the update value is the value of authentication data stored in a database of the subnet manager.

30.   (Currently Amended) The system of claim 2423 wherein:
the management port stores multiple copies of the authentication data;, and
only one copy from the multiple copies has been reset in response to the operator command.

31.   (Currently Amended) The system of claim 30 wherein the subnet manager is furtherconfigured to determine the update value for the update SMPauthentication data.

32.   (Currently Amended) The methodsystem of claim 2031 wherein the subnet manager is furtherconfigured to determine the update value by sending to the management port a read SMP requesting a current value of the authentication data maintained by the management port upon receiving the-a message indicating that the authentication data maintained by the management

15

Amendment and Response
Applicant: Norman C. Chou et al.
Serial No.: 10/057,159
Filed: January 24, 2002
Docket No.: 10011314-1/A310.258.101
Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

port has been reset, ~~receiving~~ to receive the current value of the authentication data maintained

by the management port from the management port, ~~designating~~ to designate the received value

as the update value, and ~~updating~~ to update authentication data in a database of the subnet

manager with the received value.

33.   (Currently Amended) A machine-readable medium storing a description of a circuit, ~~said~~

~~circuit~~ comprising:

     a decoder configured to ~~receive a reset signal from a configuration switch, to~~ reset an

~~copy of the~~ authentication data ~~that is~~ stored in the decoder based on a ~~in response to the~~ reset

signal received from a configuration switch, and to receive a management packet from the sub-

network (subnet) manager with an update value for the authentication data residing in a plurality

of units of an interconnect device; and

     a subnet management agent configured to receive the management packet from the

decoder and to control the update of the authentication data residing in each of the plurality of

units.

34.   (Original) A computer readable medium comprising executable instructions which when

executed on a processing system cause said process system to perform a method comprising:

     detecting that a reset of authentication data residing in a management port of the

interconnect device is required;

     informing an operator that the reset is required;

     refraining from sending subnet management packets (SMPs) to the management port

upon detecting that the reset is required;

     receiving a message from the operator that indicates that the authentication data has been

reset; and

     subsequent to the receipt of the message, sending to the management port an update SMP

with a request to set authentication data residing in each unit of the interconnect device to an

update value.

16